UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/076,254	02/12/2002	Rossmann Alain	SS-004	8579

7590 05/08/2003

Joe Zheng
SecretSEAL Inc.
7394 Wildflower Way
Cupertino, CA 95014

EXAMINER
BACKER, FIRMIN

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/08/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/076,254	Applicant(s) ALAIN ET AL.
	Examiner Firmin Backer	Art Unit 3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 February 2002* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-88* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-88* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

This is in response to a letter for patent filed on February 12th, 2002 in which claims 1-88 are presented for examination. Claims 1-88 are pending in the letter.

Preliminary Amendment

A preliminary amendment has been filed on June 17th, 2002 in which claim 1, 3-8, 13-16, 18, 20, 21, 24, 30, 31, 42-55, 60, 67, 71 and 78 have been amended. Claims 1-88 remain Pending in the letter.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-5, 10-25, 28-47 are rejected under 35 U.S.C. 102(e) as being anticipated by Pensak et al (U.S. Patent No. 6,339,825, *Applicant admitted prior art).*

3. As per claim 1, Pensak et al teach a method for providing access control management *(method for maintaining access control)* to electronic data *(electronic object such as document)*, the method comprising establishing a secured link *(established communication)* with a client *(authoring user, 108)* machine when an authentication request is received from the client machine *(see figs 1, 2, column 2 lines 49-62, 3 lines 41-47)*, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is secured in a format including security information and an encrypted data portion, the security information including access rules and controlling restrictive access to the encrypted data portion authenticating the user according to the identifier; and activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information *(see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54)*.

4. As per claim 2, Pensak et al teach a method comprising maintaining an access control management, wherein the access control management comprises a rule manager including at least one set of rules for the electronic data; and an administration interface from which the rules for a designated place for the electronic data are created, managed, or updated *(see column 6 lines 15-32)*.

5. As per claim 3, Pensak et al teach a method wherein the designated place is a folder and all files in the folder are subject to the rules *(see column 6 lines 15-32)*.

6. As per claim 4, Pensak et al teach a method wherein the designated place is a repository and all files in the repository are subject to the rules (*see column 6 lines 15-32).*

7. As per claim 5, Pensak et al teach a method wherein the rule manager provides a graphic user interface from which the rules can be created, managed or updated (*see column 6 lines 15-32).*

8. As per claim 10, Pensak et al teach a method wherein the access control management further comprises a user manager coupled to a database including a list of authorized users and respective access privileges associated with each of the authorized users (*see column 6 lines 15-32).*

9. As per claim 11, Pensak et al teach a method wherein the authenticating of the user comprises looking up in the database for the user; and getting, from the database, access location information as to where the user is authorized to access the electronic data if information about the user is located in the database (*see column 6 lines 15-32).*

10. As per claim 12, Pensak et al teach a method wherein the identifier further identifiers the client machine; and wherein the authenticating of the user comprises determining, from the access location information, whether the client machine is permitted by the user to access the electronic data (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

11. As per claim 13, Pensak et al teach a method wherein the access location information pertains to locations or specific client machines from which the user is authorized to access the electronic data (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

12. As per claim 14, Pensak et al teach a method wherein the user key is in the client machine; and wherein the activating of the user key comprises sending an authentication message to the client machine; and activating the user key with the authentication message (*see column 6 lines 38-56).*

13. As per claim 15, Pensak et al teach a method wherein the electronic data, when secured, includes a header that further includes the security information being encrypted and a signature signifying that the electronic data is secured (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

14. As per claim 16, Pensak et al teach a method wherein the security information includes a file key in addition to the access rules, and wherein the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules (*see column 6 lines 15-32).*

15. As per claim 17, Pensak et al teach a method comprising associating the activated user key with the user locally (*see figs 1, 2, column 2 lines 49-62, 3 lines 41-47).*

16. As per claim 18, Pensak et al teach a method wherein the electronic data, when secured, includes a header that includes the security information being encrypted and a signature signifying that the electronic data is secured; the encrypted security information including the access rules and a file key, and wherein the method further comprises receiving the header from the client machine, decrypting the security information in the header to retrieve the access rules therein; and retrieving the file key when the access rules are measured successfully against access privilege of the user (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

17. As per claim 19, Pensak et al teach a method further comprising sending the file key to the client machine in which the encrypted data portion can be decrypted with the file key by a cipher module executing in the client machine (*see column 7 lines3-62).*

18. As per claim 20, Pensak et al teach a method for providing access control management to electronic data, the method comprising authenticating a user attempting to access the electronic data; maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when and where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme, encrypting the security information with the public key when the electronic data is to be written into a store, and decrypting the security information with the private key when the electronic data is to be accessed by an application (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54, 7 lines3-62).*

19. As per claim 21, Pensak et al teach a method wherein the authentication of the user comprises establishing a link with a client machine from which the user is attempting to access the electronic data, demanding credential information from the user, and receiving the credential information from the client machine over the link (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

20. As per claim 22, Pensak et al teach a method wherein the credential information includes a pair of username and password provided by the user (*see figs 1, 2, column 2 lines 49-62, 3 lines 41-47).*

21. As per claim 23, Pensak et al teach a method wherein the credential information includes biometric information captured from the user by an apparatus coupled to the client machine (*see figs 1, 2, column 2 lines 49-62, 3 lines 41-47).*

22. As per claim 24, Pensak et al teach a method wherein the encrypting of the security information with the public key comprises receiving access rules and a file key, wherein the file key has been used to produce the encrypted data portion in the client machine, including the access rules and the file key into the security information; and encrypting the security information with the public key (*see column 7 lines 3-62).*

23. As per claim 25, Pensak et al teach a method comprising, generating the header with the security information encrypted therein; and uploading the header to the client machine where the header is integrated with the encrypted data portion (*see column 7 lines 3-62).*

24. As per claim 28, Pensak et al teach a method wherein the decrypting of the security information with the private key comprises receiving the header from the client machine over the link; parsing the security information from the header; and decrypting the security information with the private key (*see figs 1, 2, column 2 lines 49-62, 3 lines 41-47).*

25. As per claim 29, Pensak et al teach a method further comprising: obtaining access rules from the security information; determining whether the access rules accommodate access privilege of the user, when the determining succeeds, retrieving a file key from the security information; and sending the file key to the client machine over the link when the determining fails, sending an error message to the client machine over the link.

26. As per claim 30, Pensak et al teach a method wherein the error message indicates that the user does not have the access privilege to access the electronic data (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

27. As per claim 31, Pensak et al teach a method for providing access control management to electronic data, the method comprising receiving a request to access the electronic data; determining security nature of the electronic data; when the security nature indicates that the

electronic data is secured, the electronic data including a header and an encrypted data portion, the header including security information controlling restrictive access to the encrypted data portion and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme, determining from the security information if the user has necessary access privilege to access the encrypted data portion; and decrypting the encrypted data portion only after the user is determined to have the necessary access privilege to access the encrypted data portion (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54, 7 lines3-62).*

28. As per claim 32, Pensak et al teach a method further comprising retrieving a user key associated with a user making the request (*see column 7 lines3-62).*

29. As per claim 33, Pensak et al teach a method wherein said determining from the security information if the user has necessary access privilege comprises decrypting the security information with the user key; retrieving access rules from the security information; and measuring the access rules against the access privilege of the user (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54, 7 lines3-62).*

30. As per claim 34, Pensak et al teach a method further comprising retrieving a file key from the security information if the measuring of the access rules against the access privilege succeeds.

31. As per claim 35, Pensak et al teach a method further comprising causing the client machine to display an error message to the user if the measuring of the access rules against the access privilege fails (*see figs 1, 2, column 2 lines 49-62, 3 lines 41-47).*

32. As per claim 36, Pensak et al teach a method wherein the retrieving of the user key comprises establishing a link with a server executing an access control management; sending to the server an authentication request including an identifier identifying the user for the access control management to authenticate the user forwarding the header to the server; and receiving a file key retrieved from the header.

33. As per claim 37, Pensak et al teach a method of activating a cipher module and decrypting the encrypted data portion by the cipher module with the received file key (*see column 7 lines3-62).*

34. As per claim 38, Pensak et al teach a method comprising loading the decrypted data portion into the application (*see column 7 lines3-62).*

35. As per claim 39, Pensak et al teach a method wherein the retrieving of the user key comprises establishing a link with a server executing an access control management; sending to the server an authentication request including an identifier identifying the user for the access control management to authenticate the user, receiving an authentication message after the user

is authenticated; and activating the user key locally in the client machine (*see figs 1, 2, column 2 lines 49-62, 3 lines 41-47).*

36. As per claim 40, Pensak et al teach a method wherein the user key is in an illegible format before the activating of the user key locally in the client machine (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

37. As per claim 41, Pensak et al teach a system for providing access control management to electronic data, the method comprising a client machine executing a document securing module that operates in a path through which the electronic data is caused to pass when selected, the document securing module determining security nature of the electronic data, an access control server coupled to the client machine over a network, the access control server including an account manager managing all users who access the electronic data; and wherein the client machine and a user thereof are caused by the document securing module to be authenticated with the access control server when the security nature indicates that the electronic data is secured; and wherein access rules in the secured electronic data are retrieved with a user key associated with the user (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54, 7 lines 3-62).*

38. As per claim 42, Pensak et al teach a system wherein the access rules are measured against access privilege of the user (*see figs 1, 2, column 2 lines 49-62, 3 lines 41-47).*

39. As per claim 43, Pensak et al teach a system wherein the document securing module activates a cipher module to decrypt an encrypted data portion in the secured electronic data with a file key obtained therefrom after the document securing module determines that the access privilege of the user is permitted by the access rules (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

40. As per claim 44, Pensak et al teach a system wherein the user key stays in the access control server that receives part of the secured electronic data; and wherein the access rules and the file key are obtained from the part of the secured electronic data (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

41. As per claim 45, Pensak et al teach a system wherein the access control server forwards the file key to the client machine in a secured form over the network (*see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54).*

42. As per claim 46, Pensak et al teach a system wherein the user key stays in the client machine and is activated when both the client machine and the user are authenticated by the access control server (*see column 6 lines 15-32).*

43. As per claim 47, Pensak et al teach a system for providing access control management to electronic data, the method comprising a storage device including at least an active place designated for keeping the electronic data secured, the secured electronic data including

encrypted security information that further includes at least a set of access rules and a file key, wherein the access rules, expressed in a descriptive language, protects the file key and controls restrictive access to the secured electronic data, a client machine coupled to the storage device and executing a document securing module operative to intercept the electronic data when the electronic data is caused to transport from the active place, an access control server coupled to the client machine over a network and receiving a part of the electronic data including the encrypted security information from the client machine, the encrypted security information being decrypted with a user key associated with a user attempting to access the electronic data after both the user and the client machine are authenticated, wherein the set of access rules are measured against access privilege of the user in the access control server, if successful, the file key is returned to the client machine to facilitate a recovery of the electronic data in clear mode *(see figs 1, 2, column 2 lines 15-62, 3 lines 16-40, 5 lines 33-54, 7 lines3-62).*

Claim Rejections - 35 USC § 103

44. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

45. Claims 6-9, 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak et al. (U.S. Patent No. 6,339,825 in view of Ozog et al (U.S. PG Pub 2003/0033528).

46. As per claim 6-9, 26 and 27, Pensak et al fail to teach a method wherein parameters determining the rules from the graphic user interface are subsequently expressed in a markup language uploaded to the client machine after the user is authenticated Extensible Access Control Markup Language selected from a group consisting of HTML, XML and SGML. However, Ozog et al teach a method wherein parameters determining the rules from the graphic user interface are subsequently expressed in a markup language uploaded to the client machine after the user is authenticated Extensible Access Control Markup Language selected from a group consisting of HTML, XML and SGML (*see paragraph 0059, 0060, 0108, 0110, 0113).* Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify Pensak et al's inventive concept to include Ozog et al's a method wherein parameters determining the rules from the graphic user interface are subsequently expressed in a markup language uploaded to the client machine after the user is authenticated Extensible Access Control Markup Language selected from a group consisting of HTML, XML and SGML because this would have facilitate the viewing of the access rules.

47. As per claim 48-88, they disclose the same inventive concept as in claims 1-47, therefore, they are rejected under the same rationale.

Conclusion

48. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (*see form 892).*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-7687 for regular communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.

Firmin Backer
Examiner
Art Unit 3621

May 6, 2003